UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/637,409 | 08/11/2000 | Paul S. Henry | 1999-0785 | 7313 |

7590 03/08/2004

Samuel H Dworetsky
AT&T Corp
Post Office Box 4110
MIddletown, NJ 07748-4110

| EXAMINER | |
|---|---|
| SHERKAT, AREZOO | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/637,409 | HENRY ET AL. | |
| | Examiner | Art Unit | |
| | Arezoo Sherkat | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *11 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,13-15, and 17-20* is/are rejected.

7)☒ Claim(s) *11,12,16, and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

Claims 1-20 have been presented for examination.

### *Claim Objections*

Claim 17 is objected to because of the following informalities: in line 1, "random" should read "random number".

Appropriate correction is required.

### *Allowable Subject Matter*

Claims 11, 12, and 16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 6-10, 13-15, and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parfenov et al., (U.S. Publication No. 2002/0138728 and Parfenov hereinafter), in view of Perlman, (U.S. Patent No. 5,892,828 and Perlman hereinafter).

Regarding claim 1, Parfenov discloses a method for providing a user with access to multiple accounts (i.e., affiliate service providers) using a common password which is valid for each of the multiple accounts.

Parfenov does not expressly disclose wherein each of the multiple accounts has associated with it a unique designated password.

However, Perlman discloses wherein each of the multiple accounts has associated with it a unique designated password (i.e., user objects associate a given user with one or more application secrets, referred to as "keychains")(Col. 4, lines 31-67 and Col. 5, lines 1-55).

Furthermore, Parfenov discloses the method comprising:

generating a designated password which is to be associated with at least one of the user's multiple accounts;

receiving login information from the user for the at least one of the user's multiple accounts, wherein the login information includes a user ID belonging the user and the user's common password; and

Parfenov does not expressly disclose a designated password for each of the user's multiple accounts, which is derived form a common password provided by the user.

However, Perlman discloses determining if the user has provided valid login information based on a comparison which takes into the account the user's ID (i.e., a user name), common password (i.e., user secret/password) and the designated

password (i.e., application secret) generated for the at least one of the user's multiple accounts (Col. 4, lines 53-63 and Col. 5, lines 55-67 and Col. 6, lines 1-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include a designated password for each of the user's multiple accounts which is derived form a common password provided by the user with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 2, Parfenov does not expressly disclose wherein the designated password is generated by a hash function of the common password and some account-dependent information.

However, Perlman discloses wherein the designated password is generated by a hash function of the common password and some account-dependent information (Col. 6, lines 50-67 and Col. 7, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 3, Parfenov discloses using a symmetric key encryption algorithm (Page 3, Par. 0029).

Parfenov does not expressly disclose further comprising forming a symmetric key from the results of the hash function.

However, Perlman discloses further comprising hash function encryption algorithm (i.e., after user provides the password, the routine hashes it, if the resulting hash value matches the stored hash value, then the user is reliably authenticated)(Col. 6, lines 50-67 and Col. 7, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password using a symmetric key encryption algorithm with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 6, Parfenov discloses wherein receiving login information from the user for at least one of the user's multiple accounts, wherein the login information includes a user ID and the user's common password includes providing at least one input facility for the user to provide the user ID and common password (Page 3, Par. 0025-0026).

Regarding claim 7, Parfenov does not expressly disclose the designated password generated for the at least one of the user's multiple accounts.

However, Perlman discloses wherein determining if the user has provided valid login information based on a comparison which takes into the account the user's ID(i.e., user name), common password (i.e., user secret/password) and the designated password generated for the at least one of the user's multiple accounts (i.e., the hashed value)(Col. 4, lines 52-67) includes:

performing a hash function upon the designated password, and comparing the results of the hash function upon the designated password with a corresponding stored result to determine if a match exists (Col. 6, lines 50-67 and Col. 7, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password and comparing it with the stored hashed value with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 8, Parfenov does not expressly diclose further comprising providing access to the at least one of the user's multiple accounts if a match exists.

However, Perlman discloses further comprising providing access to the at least one of the user's multiple accounts if a match exists (Col. 7, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password, comparing it with the stored hashed value, and providing access if a match exists with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 9, Parfenov does not expressly disclose wherein determining if the user has provided valid login information based on a comparison which takes into the account the user's ID, common password and the designated password generated for the at least one of the user's multiple accounts.

However, Perlman discloses wherein determining if the user has provided valid login information based on a comparison which takes into the account the user's ID, common password and the designated password generated for the at least one of the user's multiple accounts includes:

calculating the designated password (i.e., hashed value of the password) according to a password transform algorithm (i.e., hash function)(Col. 3, lines 34-49).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 10, Parfenov discloses a method for providing access to multiple online accounts via a common password, the method comprising: receiving a common password associated with an online account; and

parfenov does not expressly disclose generating the designated password.

However, Perlman discloses determining if the universal password is valid for the associated online account based upon a designated password which was previously generated for the associated online account, wherein the designated password was previously generated based upon a password transform calculation (i.e., hash function)(Col. 6, lines 18-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in

a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 13, Parfenov does not expressly disclose generating a designated password.

However, Perlman discloses further comprising:

generating a designated password (i.e., application secrets for pre-determined application programs) for each of the multiple online accounts which is accessible via the common password (Col, 4, lines 53-67 and Col. 5, lines 1-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 14, Parfenov does not expressly disclose generating a designated password for the user's for each of the multiple online accounts.

However, Perlman discloses a method for providing access to multiple Web accounts via a universal password which is valid for the multiple Web accounts, the method comprising:

providing a designated password for each of the multiple Web accounts, receiving the universal password for access to at least one of the multiple Web accounts (Col. 4, lines 53-67 and Col. 5, lines 1-55);

determining if the universal password (i.e., user secret/password) is valid based on the associated designated password for the at least one of the multiple Web accounts (Col. 6, lines 18-67 and Col. 7, lines 1-10); and

providing access to the at least one of the multiple Web accounts provided the universal password is valid (Col. 5, lines 55-67 and Col. 6, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts for her/him to access various services and applications in a distributed network system by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 15, Parfenov does not expressly disclose the designated password calculated from a hash function.

However, Perlman discloses wherein the designated password is calculated for each of the multiple Web accounts (i.e., authenticating a user to various services and applications in a distributed network system) based on a hash function which

incorporates the universal password as an input to the hash function (Col. 6, lines 18-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts for her/him to access various services and applications in a distributed network system by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Regarding claim 19, Parfenov does not expressly disclose the designated password calculated from a hash function.

However, Perlman discloses further comprising: providing a new designated password for the at least one of the multiple Web accounts if requested (i.e., requesting through user login)(Col. 4, lines 53-67 and Col. 5, lines 1-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov with the teachings of Perlman to include generating a designated password for each of the user's multiple accounts by implementing a hash function to the user's common password with the motivation to dynamically authenticating a user to various services and applications in

a distributed network system using a single common password (Perlman, Col. 3, lines 27-30).

Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parfenov et al., (U.S. Publication No. 2002/0138728 and Parfenov hereinafter) and Perlman, (U.S. Patent No. 5,892,828 and Perlman hereinafter), in view of Gressel et al., (U.S. Patent No.5,664,017 and Gressel hereinafter).

Regarding claim 4, Parfenov or Perlman does not expressly disclose wherein the symmetric key is used to encrypt the random number.

However, Gressel discloses wherein the symmetric key is used to encrypt the random number (Col. 9, lines 38-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov and Perlman with the teachings of Gressel to include an encrypted random number in the authentication process with the motivation to provide an improved method and apparatus for international and national encryption and decryption of sensitive data so as to preserve confidentiality and message integrity (Gressel, Col. 2, lines 7-11).

Regarding claim 5, Parfenov or Perlman does not disclose wherein the random number is encrypted via a symmetric encryption algorithm.

However, Gressel discloses wherein the random number is encrypted via a symmetric encryption algorithm (Col. 9, lines 38-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov and Perlman with the teachings of Gressel to include an encrypted random number in the authentication process with the motivation to provide an improved method and apparatus for international and national encryption and decryption of sensitive data so as to preserve confidentiality and message integrity (Gressel, Col. 2, lines 7-11).

Claims 17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parfenov et al., (U.S. Publication No. 2002/0138728 and Parfenov hereinafter) and Perlman, (U.S. Patent No. 5,892,828 and Perlman hereinafter), in view of Nguyen, (U.S. Patent No. 5,689,566 and Nguyen hereinafter).

Regarding claim 17, Parfenov does not expressly disclose generating designated passwords using hash functions.

Perlman discloses using hash functions to dynamically authenticate a user to various services and applications in a distributed network system using a single common password (Col. 3, lines 27-30).

Perlman does not expressly disclose incorporating a random number as an input to the hash function.

However, Nguyen discloses wherein the hash function also incorporates a random number as an input to the hash function (Col. 4, lines 10-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov and Perlman with the teachings of Nguyen to manipulate random numbers with a hash function with the motivation to ensure that access to data is restricted to authorized parties while at the same time providing more consistent performance (Nguyen, Col. 1, lines 60-65).

Regarding claim 20, Parfenov does not expressly disclose generating a designated password using a hash function.

Perlman does not expressly disclose calculating the new designated password using the universal password and a random number.

However, Nguyen discloses wherein providing a new designated password for the at least one of the multiple Web accounts if requested includes:

generating a random number, and calculating the new designated password (i.e., CRC signature) based on at least the universal password (i.e., a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard, SHS) and the random number (Col. 4, lines 10-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov and Perlman with the teachings of Nguyen to manipulate random numbers with a hash function with the

motivation to ensure that access to data is restricted to authorized parties while at the same time providing more consistent performance (Nguyen, Col. 1, lines 60-65).

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Parfenov et al., (U.S. Publication No. 2002/0138728 and Parfenov hereinafter) and Perlman, (U.S. Patent No. 5,892,828 and Perlman hereinafter), in view of Abraham, (U.S. Patent No. 6,606,387 and Abraham hereinafter).

Regarding claim 18, Parfenov does not expressly disclose generating a designated password based on a universal password.

Perlman discloses wherein determining if the universal password (i.e., user secret/password) is valid based on the associated designated password (i.e., application secret associated with the user) for the at least one of the multiple Web accounts includes:

receiving a user ID (i.e., user name during login)(Col. 4, lines 53-65);

receiving the associated designated password, and comparing the received associated designated password with a corresponding saved designated password for the at least one of the multiple Web accounts (Col. 6, lines 50-67 and Col. 7, lines 1-10);

Perlman does not expressly disclose retrieving an encrypted random number based on the user ID.

However, Abraham discloses:

retrieving an encrypted random number based on the user ID (i.e., unique reference numbers)(Col. 8, lines 3-26).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Parfenov and Perlman with the teachings of Abraham to include retrieving an encrypted random number based on the user id (i.e., unique reference numbers) with the motivation to provide a system and method for securely establishing a cryptographic key between a first cryptographic device and a second cryptographic device wherein a plurality of unrelated random numbers are distributed to serve as key components and for ensuring a high probability that a cryptographic key established between a first cryptographic device and a second cryptographic device is unique (Abraham, Col. 2, lines 57-67).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Technology Center 2100
March 4, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100